Information Systems Audit Photocopier Data Security

Presented to the ITMC

By

Warren Dupuis

The Issue

- Photocopiers can have hard drives just like computers, and thus may store sensitive and confidential data internally.

- If not properly controlled, there is potential for unauthorized access to this data.

- Although the audit did not identify any data security breaches, there is a lack of awareness of data security controls.

Conclusion

- While agencies reviewed were aware of settings to force automatic removal of all stored data, some agencies store data on copier hard drives potentially allowing unauthorized access to data. However, data was either protected by a required username/password or copiers were set to automatically removed stored data.

Recommendation #1

- Department of Administration update all photocopier pool contracts to contain security and hard drive management requirements.

- Response: Concur

  - The Department will amend all photocopier pool contracts to ensure agencies properly configure photocopiers to automatically remove data from hard drives at the time of use. Further, photocopier pool contracts will specify that data must be erased or the hard drive removed when a photocopier is replaced.

Recommendation #2

- Department of Administration use existing IT Groups to facilitate awareness of state data security policy.

- Response: Concur
  - The Department will continue to use the Information Security Manages Group, the Information Technology Managers Council, and the Information Technology Board to Facilitate awareness of state data security policy.

Recommendation #2 (cont.)

- Department of Administration use existing IT Groups to facilitate awareness of state data security policy.

- Response: Concur

  – In addition, the Department will continue to us the information Security Managers Group at its quarterly workshops and the annual Information Technology Conference to increase information security awareness including *media storage issues.*

Questions?